AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in this application:

Listing of claims:

Claims 1-24 (Canceled)

25. (New) A method of protecting a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate and a selected image content;

selecting an authentication mode for processing the extracted feature values, the processing of the extracted feature values comprising deriving data corresponding to the extracted feature values based on the selected authentication mode; and

creating an image signature based on the data corresponding to the feature values.

26. (New) The method as claimed in claim 25, wherein the processing comprises correcting coding (ECC) the extracted feature values to derive the data corresponding to the feature values.

27. (New) The method as claimed in claim 25, wherein the feature values from each of a plurality of codeblocks of the original digital image are thresholded and coded to create the data corresponding to the feature values.

28. (New) The method as claimed in any one of claim 25, wherein the processing further comprises embedding the data corresponding to the feature values into the digital image.

29.(New) The method as claimed in claim 26, further comprising applying ECC coding again to parity check bits generated during the ECC coding of the extracted feature values to generate the data corresponding to the feature values.

30.(New) The method as claimed in claim 28, wherein the embedding of the data corresponding to the feature values as a watermark is conducted in a lossy or a lossless way, based on the selected authentication mode.

31.(New) The method as claimed in any one of claim 25, wherein the creating of the image signature comprises applying a cryptographic hashing function to a bit sequence representing the data corresponding to the feature values.

32. (New) The method as claimed in any one of claim 25, wherein the creating of the image signature comprises utilising a private key.

33. (New) The method as claimed in any one of claim 25, wherein the method further comprises distributing the digital image, including the embedded data, as the authentic digital image.

34. (New) The method as claimed in any one of claim 25, further comprising coding the digital image, including the embedded data, utilising JPEG2000 compression.

35. (New) The method as claimed in claim 34, wherein the extracting of the feature values, the embedding of the data corresponding to the feature values, and the creating of the image signature are performed as part of the JPEG 2000 coding.

36. (New) A method of authenticating a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate; and

processing the extracted feature values to derive data corresponding to original feature values based on a selected authentication mode; and comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

37. (New) The method as claimed in claim 36, wherein deriving the data corresponding to the feature values comprises ECC coding the extracted data and extracted feature values.

38. (New) The method as claimed in claim 36, wherein the extracted feature values from each of a plurality of codeblocks of the digital image are decoded to derive the data corresponding to the original feature values.

39. (New) The method as claimed in any one of claim 36, further comprising extracting data embedded as a watermark in the digital image; and the processing the extracted data and the extracted feature values to derive the data corresponding to original feature values.

40. (New) The method as claimed in claim 37, further comprising applying ECC decoding twice to the extracted data.

41. (New) The method as claimed in claim 35, wherein the data is embedded in a lossy or lossless way as a watermark in the digital image.

42. (New) The method as claimed in any one of claim 36, further comprising applying a cryptographic technique to the image signature to derive a bit sequence representing the reference data.

43. (New) The method as claimed in any one of claim 36, further comprising applying a public key to process the image signature for deriving the reference data.

44. (New) The method as claimed in any one of claim 36, wherein the method further comprises receiving the digital image as a coded digital image.

45. (New) The method as claimed in claim 44, wherein the digital image is coded utilising JPEG2000.

46. (New) The method as claimed in claim 36, wherein the extracting of the data embedded as a watermark, the extracting of feature values from the digital image, the processing of the extracted data and extracted feature values, and the comparing of the derived data corresponding to the original feature values with the reference data are performed as part of the JPEG 2000 de-coding.

47. (New) A system for protecting a digital image, the system comprising:

a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate;

a mode selector for selecting an authentication mode for processing the extracted feature values;

a processor device for deriving data corresponding to the extracted feature values based on the selected authentication mode; and

wherein the processor device further creates an image signature based on the data corresponding to the feature values.

48. (New) A computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of protecting a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate;

selecting an authentication mode for processing the extracted feature values, the processing of the extracted feature values comprising deriving data corresponding to the extracted feature values based on the selected authentication mode; and

creating an image signature based on the data corresponding to the feature values.

49. (New) A system for authenticating a digital image, the system comprising:

a feature value extractor device for extracting feature values from the digital image based on a selected authentication bit-rate;

a processor device for processing the extracted feature values based on a selected authentication mode to derive data corresponding to original feature values and for comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.

50. (New) A computer readable data storage medium having stored thereon computer program code means for instructing a computer to execute a method of authenticating a digital image, the method comprising:

extracting feature values from the digital image based on a selected authentication bit-rate;

processing the extracted feature values based on a selected authentication mode to derive data corresponding to original feature values; and

comparing the derived data corresponding to the original feature values with reference data derived from an image signature associated with the digital image.